Impossibility Theorems and the Universal Algebraic Toolkit

Mario Szegedy and Yixin Xu
Department of Computer Science
Rutgers, The State University of New Jersey

szegedy/yixinxu @cs.rutgers.edu

June 4, 2015

Abstract

We elucidate a close connection between the Theory of Judgment Aggregation (more generally, Evaluation Aggregation), and a relatively young but rapidly growing field of universal algebra, that was primarily developed to investigate constraint satisfaction problems. Our connection yields a full classification of non-binary evaluations into possibility and impossibility domains both under the idempotent and the supportive conditions. Prior to the current result E. Dokow and R. Holzman nearly classified non-binary evaluations in the supportive case, by combinatorial means. The algebraic approach gives us new insights to the easier binary case as well, which had been fully classified by the above authors. Our algebraic view lets us put forth a suggestion about a strengthening of the Non-dictatorship criterion, that helps us avoid "outliers" like the affine subspace. Finally, we give upper bounds on the complexity of computing if a domain is impossible or not (to our best knowledge no finite time bounds were given earlier).

Keywords: *Judgment aggregation, Discursive dilemma, Condorcet's paradox, Arrow's impossibility theorem, Social choice theory, Dictatorship, Compatible operations, Constraint satisfaction problems, Dichotomy, Polymorphisms*

1 Introduction

The goal of Judgment Aggregation is to investigate the existence or nonexistence of functions that "aggregate individual sets of judgments on multiple, logically connected propositions into collective sets of judgments" [LP02]. Arrow's impossibility theorem, which can be interpreted in the judgment aggregation framework, is a powerful example showing that even in simple cases we cannot meaningfully aggregate individual opinions into a social opinion.

Elad Dokow and Ron Holzman [DH10a, DH10b] have studied an elegant generalization of Judgment Aggregation, that we call after their title *Aggregation of Evaluations*. Let J be a finite set of issues and D be a finite set of possible positions/opinions (like 'yes', 'no' etc.). Without loss of generality we assume that

$$J = [m] = \{1, \ldots, m\}.$$

An evaluation $(v_1, \ldots, v_m) \in D^m$ assigns a position in D to each $j \in [m]$. The binary case, when $D = \{0, 1\}$ has received special attention [Wil75, RF86, DH10a]. Our fundamental object is the *domain* $X \subseteq D^m$ of *feasible evaluations*, these are the evaluations (i.e. opinion-combinations) that we allow for the voters to choose from.

Example 1. Assume that during a murder trial the members of the jury have to vote on two issues: 1. the suspect had a knife; 2. the suspect was the murderer; with taking a position either 'yes' or 'no' on each of the issues. Each member must take a position on both issues, but the jury agrees that the position-combination (1: no, 2: yes) should not be valid: neither as an individual vote nor when we *aggregate* the votes. Thus $X = \{(\text{no,no}), (\text{yes,no}), (\text{yes,yes})\}$.

Aggregators. When n members of a society take a position on all of the m issues, and each member's vote is from X, we get a *profile* vector

$$(x^{(1)}, \ldots, x^{(n)}) \in X^n.$$

Our goal is to design a function $f : X^n \to X$ that takes profile vectors into single elements of X. Such functions are called *aggregators*. The aggregators we shall consider must satisfy three conditions that come directly from Arrow's famous conditions, he has identified while studying the special case of preference list aggregation. Before we describe them we remark that

$$x^{(i)} = (x_1^{(i)}, \ldots, x_m^{(i)}) \in D^m \quad \text{for } i = 1, \cdots, n,$$

are vectors themselves: $x_j^{(i)}$ is the ith voter position on the jth issue. Thus the profile is a vector of vectors. The output of f is a vector in D^m, representing the aggregated positions on the m issues. The latter vector must also belong to X.

The first and key condition is that each issue ought to be aggregated independently from the others (also called point-wise aggregation or Issue by Issue Aggregation):

Issue-by-Issue Aggregation (IIA): There are functions $f_j : D^n \to D$ ($1 \le j \le m$) such that for every $(x^{(1)}, \ldots, x^{(n)}) \in X^n$:

$$f(x^{(1)}, \ldots, x^{(n)}) = \left(f_1\left(x_1^{(1)}, \ldots, x_1^{(n)} \right), \ldots, f_m\left(x_m^{(1)}, \ldots, x_m^{(n)} \right) \right)$$

There is a nice way to visualize the IIA property via the picture

$$
\begin{array}{cccccc}
x_1^{(1)} & \cdots & x_m^{(1)} & \in & X \\
& \vdots & \\
x_1^{(n)} & \cdots & x_m^{(n)} & \in & X \\
\hline
\downarrow_{f_1} & \cdots & \downarrow_{f_m} & \\
x_1 & \cdots & x_m & \in & X
\end{array}
$$

Above we aggregate column j (where $j \in [m]$ is an issue) by function f_j. The condition that f takes X^n to X is equivalent to saying that if each row belongs to X, then so does the aggregated row. The component aggregate functions should work in unison to accomplish this. We have adopted the term "Issue by Issue Aggregation" coined by E. Dokow and R. Holzman [DH10a, DH10b], which is in this generalized context more fitting than the commonly used "Independence of Irrelevant Alternatives" expression, with the benefit that the acronym remains the same.

Uniqueness of the IIA decomposition. The representation of $f : X^n \to X$ as $(f_1, \ldots, f_m)$ is clearly not unique for instance when D contains any element that does not occur as a constituent in any $x \in X$. In order to avoid non-uniqueness of the f_js we define

$$
D_j = \mathrm{pr}_j X = \{u_j \mid (u_1, \ldots, u_m) \in X\}.
$$

If we define f_j on D_j^n instead of D^n, it is easy to see that f_j becomes unique. Throughout the paper we shall assume this.

Next we describe the two other conditions (besides IIA) Arrow has imposed on an aggregator $f : X^n \to X$.

Idempotency (or Unanimity): $f(x, \ldots, x) = x$ for every $x \in X$.

Lemma 1. *An IIA aggregator $f = (f_1, \ldots, f_m)$ is idempotent if and only if every f_j is idempotent in the universal algebraic sense, i.e.*

$$
\forall \, 1 \leq j \leq m \quad \forall \, u \in D_j : \qquad f_j(u, \ldots, u) = u
$$

Non-dictatorship: Aggregator $f : X^n \to X$ is a dictatorship if there is a $1 \leq k \leq n$ such that for every $(x^{(1)}, \ldots, x^{(n)}) \in X^n$ we have $f(x^{(1)}, \ldots, x^{(n)}) = x^{(k)}$. Otherwise the Non-dictatorship condition holds for f.

Lemma 2. *An IIA aggregator $f = (f_1, \ldots, f_m)$ is a dictatorship if and only if there is a $1 \leq k \leq m$ such that each f_j is a* projection *on the kth coordinate in the universal algebraic sense:*

$$
\forall \, 1 \leq j \leq m \quad \forall \, u_1, \ldots, u_n \in D_j : \qquad f_j(u_1, \ldots, u_n) = u_k
$$

Definition 1 (Impossibility/Possibility domains). We call an $X \subseteq D^m$ a possibility domain (after Arrow) with respect to the IIA + Idempotency + Non-dictatorship conditions if for some $n \geq 2$ an aggregator function f for X with arity n exists that satisfies the three said conditions. Otherwise X is an impossibility domain.

In this article we completely characterize impossibility domains with respect to the IIA + Idempotency + Non-dictatorship and also for the case when Idempotency is replaced with

Supportiveness: $f : X^n \to X$ is supportive if for every $x^{(1)}, \ldots, x^{(n)} \in X^n$ and every $1 \le j \le m$ we have that $f(x^{(1)}, \ldots, x^{(n)})_j \in \{x_j^{(1)}, \ldots, x_j^{(n)}\}$.

Lemma 3. *An IIA aggregator $f = (f_1, \ldots, f_m)$ is a supportive if and only if every f_j is conservative in the universal algebraic sense:*

$$\forall\, 1 \le j \le m \qquad \forall\, u_1, \ldots, u_n \in D_j : \qquad f_j(u_1, \ldots, u_n) \in \{u_1, \ldots, u_n\}$$

Supportiveness implies Idempotency, but not vice versa.

Prior to our result a full characterization of all impossible binary domains was obtained under IIA + Idempotency + Non-dictatorship in [DH10a]. They have extended their work to the non-binary case, but have obtained only a partial characterization, and only under the IIA + Supportiveness + Non-dictatorship conditions.

In our characterization we exploit a Galois Connection discovered by D. Geiger [Gei68]. Geiger's duality theorem allows us to characterize the nonexistence of aggregators with existence of gadgets — existential logical expressions created from X and a few very basic relations, like assignment giving or unary relations. (Gadgets are also sometimes called conjunctive queries in the literature.) Our main results are stated in Theorem 8 and Theorem 17. Our main contribution is not any new technology but rather pointing to a so far unexplored very broad connection. Simplicity only works to the new connection's favor.

Based on the algebraic view, we are also in the position to strengthen the Non-dictatorship condition to exclude the possibility of what experts agree are outliers such as linear subspaces.

The theory we use here is getting increasingly familiar to computer scientists because it gives a powerful machinery to tackle the well-known dichotomy conjecture of Feder and Vardy [FV98] for Constraint Satisfaction Problems (CSP). The hope is that the connection will allow researchers to exploit the vast material that CSP research has created, in proving impossibility theorems.

2 Background

The elegant general combinatorial framework described in the introduction which serves as the basis of the current paper was laid down by E. Dokow and and R. Holzman in [DH10a, DH10b]. We have named it "Aggregation of Evaluations" after their titles. In their two breakthrough results they make decisive advances towards classifying impossibility domains, i.e. those X from which we cannot aggregate opinions. In particular, they completely settle the binary case. To explain their results we need some definitions.

Definition 2. We call X non-degenerate if $|\mathrm{pr}_j X| > 1$ for every $1 \le j \le m$. Since the issues where degeneration occurs can be trivially aggregated, without loss of generality we can assume that X is non-degenerate.

Definition 3 (Blockedness graph and MIPE)**.** The blockedness graph for domain $X \subseteq \{0,1\}^m$ is the following directed graph on the vertex set $V = [m] \times \{0,1\}$: There is a directed edge from $(k, \sigma) \in V$ to $(\ell, \rho) \in V$ where $k \ne \ell$ if and only if there are: (i.) a subset $S \subseteq [m]$ such that $k, \ell \in S$ and (ii.) a (partial-)evaluation $u : S \to \{0,1\}$ with $u_k = \sigma$ and $u_\ell = \neg\rho$ such that there is no extension of u to any full evaluation x in X, but if we flip any bit of u then the resulting partial evaluation extends to some element of X. The above partial assignment u is called a MIPE (minimally infeasible partial evaluation).

Definition 4 (Total blockedness). Domain $X \subseteq \{0,1\}^m$ has the total blockedness condition if and only if the blockedness graph is strongly connected.

A result leading to [DH10a] was that of Nehring and Puppe [NP02]. They have obtained a complete classification of binary impossibility domains, when a monotonicity condition is added to the usual conditions. An aggregator is said to be monotone if for every issue j in any situation the aggregate position on issue j does not change if a voter decides to switch his/her position on the jth issue to the current aggregate position.

Theorem 4 (Nehring and Puppe [NP02]). *A non-degenerate $X \subseteq \{0,1\}^m$ is an impossibility domain with respect to IIA + Idempotency + Monotonicity + Non-dictatorship if and only if X is totally blocked.*

The complete characterization of binary evaluations without the monotonicity condition was finally given by E. Dokow and R. Holzman:

Theorem 5 (E. Dokow, R. Holzman [DH10a]). *Let $X \subseteq \{0,1\}^m$, non degenerate. Then X is an impossibility domain with respect to IIA + Idempotency + Non-dictatorship if and only if X is totally blocked and is not an affine subspace.*

Dokow and Holzman has also made significant progress for general D [DH10b]. In their near-characterization they use a generalization of total blockedness for non-binary predicates, which is similar but more intricate than the binary notion, and we postpone the definition to Section 10.1 (Definition 17).

We also need to define a condition on a relation X, which is called 2-decomposability in the universal algebra literature. We have adopted this term rather than the "not multiply constrained" expression for the same concept in [DH10b].

Definition 5. For an m-ary relation X on D and for $1 \le k < \ell \le m$, let $\mathrm{pr}_{k,\ell}X = \{(u_k, u_\ell) \mid (u_1, \ldots, u_m) \in X\}$. A relation X is called 2-decomposable if, for any tuple $x = (x_1, \ldots, x_m) \in D^m$ we have $x \in X$ if and only if $(x_k, x_\ell) \in \mathrm{pr}_{k,\ell}X$ for all $1 \le k < \ell \le m$.

Remark 1. Coincidentally, in [DH10b] the '2-decomposable' expression also occurs, but with a very different meaning.

Theorem 6 (E. Dokow, R. Holzman [DH10b]). *Let $X \subseteq D^m$, non-degenerate and non-binary (there is a $1 \le j \le m$ such that $|\mathrm{pr}_j X| > 2$). If X is totally blocked and not 2-decomposable (see Definition 5) then X is an impossibility domain with respect to IIA + Supportiveness + Non-dictatorship.*

Theorem 7 (E. Dokow, R. Holzman [DH10b]). *Let $X \subseteq D^m$. If X is non-degenerate and not totally blocked then X is a possibility domain with respect to IIA + Supportiveness + Non-dictatorship.*

3 Our Results

In spite of the impressive advances due to Dokow and Holzman, important questions have remained open: 1. Complete the characterization of the Supportive case, when $|D| > 3$. (In [DH10b] the case $|D| = 3$ is resolved.) 2. Settle the $|D| > 2$ case with the Idempotency condition.
We take the inspiration from the algebraic theory and combine it with ideas from [DH10b] to get a full characterization of the non-binary case, with the Supportiveness and the Idempotency conditions.

Theorem 8. *Let $X \subseteq D^m$, non-degenerate and non-binary. If X is totally blocked then X is an impossibility domain with respect to IIA + Supportiveness (Idempotent) + Non-dictatorship if and only if there is no Supportive (Idempotent) non-dictatorial IIA aggregator with at most three ($|D|$) voters.*

The characterization (to our knowledge for the first time) allows for an algorithmic determination if X is an impossibility domain with respect to the Supportive (Idempotent) conditions.

Gadgets. It turns out that we can characterize impossibility domains in a dual way, in terms of a set of *gadgets*. Our new characterization, that provides *witnesses* to impossibility, has not been known earlier in the voting theory context. Gadgets (or *conjunctive queries*) are expressions used in reductions between constraint satisfaction problems when we translate instances locally (term by term). They are existentially quantified conjuncts of clauses, where each clause is a relation. The relations in this interpretation are viewed as Boolean-valued functions on not necessarily Boolean *variables*. The syntax of a gadget is:

$$R(\vec{x}) = \exists \vec{y} : \ S_1(\vec{x}, \vec{y}) \wedge \ldots \wedge S_k(\vec{x}, \vec{y}) \quad \text{(each } S_i \text{ in effect depends only on subsets of } \vec{x}, \vec{y})$$

Their purpose is to express new relations from a given set of relations.

A theorem of D. Geiger [Gei68] establishes a connection between the nonexistence of aggregators for a set Γ of relations and the existence of Γ-gadgets (i.e. in which all relations are from Γ or the '=' relation). This theorem serves as the backbone of the algebraic theory of constraint satisfaction problems developed by P. Jeavons, A. A. Bulatov, A. A. Krokhin, D. A. Cohen, M. Cooper, M. Gyssens [JCG97, Jea98, JCC98, BJK05] and several other researchers.
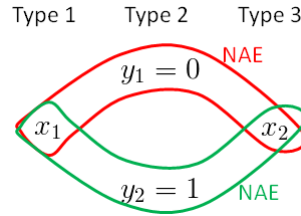

Figure 1: The multi-sorted Not All Equal (NAE) gadget to express the multi-sorted inequality relation between x_1 (type 1) and x_2 (type 3). Variables y_1 and y_2 are existentially bound (and they are also set to constant). This gadget is central in our proof of Arrow's theorem.

This is our starting point too. In universal algebra (IIA) aggregators are called *polymorphisms*. They differ from the aggregators in our introduction in that they are single-sorted: $f_1 = f_2 = \ldots = f_m$. *Multi-sorted* polymorphisms, i.e. when the f_js can be different, have also been studied in the algebraic literature [BJ03, Bul11]. When dealing with multi-sorted polymorphisms, all relations and gadgets must be multi-sorted as well. In the multi-sorted world first we must declare a type for every variable. The typing of the variables serves the same purpose as in programming languages: when a function is called, the types of the called variables must match with the types in the function declaration. In the same spirit, every multi-sorted l-ary relation R we construct (or given to us) must come with a sequence of l (not necessarily different) types. We may call this type declaration. The typing must be consistent: the the types of the variables involved in any occurrence of a relation in a gadget must match with the type declaration.

In this article we prove a multi-sorted version of Geiger's theorem (see Section 4). This allows us to prove impossibility results simply by producing sets of gadgets. If we want to prove that $X \subseteq \prod_j^m D_j$ is an impossibility domain, we need to construct X^+-gadgets for a certain "complete" set of (multi-sorted) relations. Here the '+' in the upper index refers to the permission to use assignment-giving relations (i.e. '$x = a$,' where $a \in D_j$, for type j variables) in our gadgets in addition to X. In all cases X must be viewed as a multi-sorted relation, all components (arguments) having different types. The Idempotency constraint is encoded in the '+' of X^+. Alternatively, the Supportiveness condition in the gadget-reformulation translates to the permission of using arbitrary unary relations in the gadgets. When we allow the latter, the gadget is an $X^{\mho}$-gadget.

Theorem 9. *For every D and m there is a fixed finite set $\mathcal{P} = \mathcal{P}(D, m)$ of multi-sorted relations such that $X \subseteq D^m$ is an impossibility domain with respect to IIA + Idempotency (Supportiveness) + Non-dictatorship if and only if we can express every member of $\mathcal{P}$ with a gadget whose conjunct has only (appropriately multi-sorted) X^+- ($X^{\mho}$)-clauses. In addition, the number of auxiliary variables is upper bounded by some explicit function $\phi(m, |D|)$ (single exponential in m).*

The theorem in more details is restated in Theorem 17 and proved in section 6.

Our characterizations allow us to compute in finite time if X is an impossibility domain (both in the Idempotent and in Supportive cases) in two different ways: either by checking aggregators up to a certain number of arguments (Theorem 8), or by checking gadgets up to a certain size (Theorem 9).

One of the main applications of our gadget characterization is that we can prove the impossibility of a domain X by merely presenting a few gadgets (rather than trying to exclude a large set of aggregators). In some cases we can tailor the gadgets to the specific problem, exploiting symmetries. A combined approach where we exclude most aggregators by gadgets while the rest we treat directly is also possible. Using gadgets we can show that the Pairwise Distinctness relation defined by

$$\{(u_1, \ldots, u_m) \in D^m \mid u_k \neq u_\ell \, (1 \leq k < \ell \leq m)\}$$

is an impossibility domain when $|D| > m \geq 2$ and when $|D| = m \geq 3$ with respect to the IIA + Idempotency + Non-dictatorship conditions. In [DH10b] this is proven only under the IIA + Supportiveness + Non-dictatorship conditions, and [FF11] proves the above only when $|D| = m > 2$.

The possibility notion we have discussed is considered too generous by some authors. Several further restrictions were studied e.g. [Kal02]. Dokow and Holzman, for instance, question if linear subspaces of $\{0, 1\}^m$ that emerge in Theorem 5 should really be considered possibility domains [DH10a]. In Section 12 we propose a new aggregator class that strengthens the notion of Non-dictatorship. Our new definition directly comes from the algebraic theory and has many desirable properties.

Although the case of binary evaluations was completely settled by Dokow and Holzman, universal algebra gives a tad more refined form of their theorem:

Theorem 10. *Let $X \subseteq \{0, 1\}^m$ non-degenerate. Then X is an impossibility domain with respect to IIA + Idempotency + Non-dictatorship if and only if X is totally blocked and it is not an affine subspace. If X is not totally blocked then for all $1 \leq j \leq m$ one of the following holds:*

1. *there is an f such that f_j is the semi-lattice operation $u \vee v$ or $u \wedge v$,*

2. *there is an f such that f_j is the majority operation $(u \vee v) \wedge (v \vee w) \wedge (w \vee u)$,*

3. *there is an f such that f_j is the Mal'tsev operation $u - v + w \mod 2$,*

4. *f_j is a dictatorship for every f.*

4 The algebraic theory

A key observation is that the algebraic theory can be made work in the assignment aggregation context if we turn to *multi-sorted* relations, gadgets, polymorphisms, etc. instead of the more usual single-sorted ones.

Multi-sorted relations differ from usual relations in that each component of the relation we consider has a type. Each type b has a designated range set D_b. Without loss of generality we may assume that the set of permissible types is $[t] = \{1, \ldots, t\}$ where t is a fixed positive integer. The corresponding ranges are $D_1, \ldots, D_t$. Let $X \subseteq \prod_{j=1}^m D_{\tau_j}$ where $\tau_j \in [t]$ for $1 \leq j \leq m$. We denote X with (X, τ), where $\tau = (\tau_1, \ldots, \tau_m)$, to indicate both that it is multi-sorted and the types of its components. (In our assignment aggregation setting $t = m$, $D_j = \mathrm{pr}_j X$ and the typing of X will be $(X, (1, \ldots, m))$.)

Definition 6 (gadgets, multi-sorted). We fix a type set $[t]$, $\{D_b\}_{b \in [t]}$. A multi-sorted relation (R, τ) multi-sorted gadget-reduces to a set Γ of multi-sorted relations if there is a multi-sorted gadget expression

$$R(x_1, \ldots, x_k) = \exists y_1, \ldots, y_{k'} :\ R_1(z_{1,1}, \ldots, z_{1,k_1}) \wedge \ldots \wedge R_p(z_{p,1}, \ldots, z_{p,k_p})$$

where each R_i is either from Γ or the multi-sorted equality relation $(x = y, (\mathrm{b,b}))$ (so $\mathrm{type}(x) = \mathrm{type}(y) = b$) for some $b \in [t]$. Variables $z_{1,1}, \ldots, z_{p,k_p}$ are from the set $\{x_1, \ldots, x_k\} \cup \{y_1, \ldots, y_{k'}\}$.

In the algebraic theory of CSPs voting functions are called polymorphisms. They are very extensively studied and classified according to their algebraic properties. In the more usual single-sorted case we are forced to aggregate each issue with the same function. In the multi-sorted case different types are aggregated independently: we have as many aggregator functions as types. (Even when for two types $a \neq b$ we have $D_a = D_b$, aggregators f_a and f_b may differ.) These are exactly the polymorphisms we need in the evaluation aggregation setting.

Definition 7 (multi-sorted polymorphism). Fix t, $\{D_b\}_{b \in [t]}$. Let (X, τ) be a multi-sorted relation where $\tau = (\tau_1, \ldots, \tau_m) \in [t]^m$. Fix $n \geq 1$. A collection $f_b : D_b^n \to D_b$ $(1 \leq b \leq t)$ of functions is said to be a multi-sorted polymorphism of (X, τ) if the tuple $(f_{\tau_1}, \ldots, f_{\tau_m})$ is an IIA aggregator for relation X, i.e. it takes X^n into X. More generally, a collection $f_b : D_b^n \to D_b$ $(1 \leq b \leq t)$ of functions is a multi-sorted polymorphism with respect to a set Γ of multi-sorted relations (each relation is over the same fixed set of types) if $\{f_b\}_{b \in [t]}$ is a multi-sorted polymorphism for each relation in Γ.

Note. The above generalizes the notion of single sorted polymorphism, when $t = 1$ and $D_1 = D$, and also the IIA aggregators of the introduction with the choice $t = m$, $D_j = \mathrm{Pr}_j(X)$, and with typing X as $(X, (1, \ldots, m))$.

Definition 8 (MPol). Fix $[t]$ and $\{D_b\}_{b \in [t]}$. The set of *all* multi-sorted polymorphisms for a set Γ of multi-sorted relations is denoted by $\mathrm{MPol}(\Gamma)$.

Definition 9 (MInv). Fix $[t]$ and $\{D_b\}_{b \in [t]}$. The set of *all* multi-sorted relations that are kept by a set $\mathcal{F}$ of multi-sorted aggregator functions is denoted by $\mathrm{MInv}(\mathcal{F})$.

Definition 10 ($\langle \cdot \rangle$). Fix $[t]$ and $\{D_b\}_{b \in [t]}$. For a set Γ of multi-sorted relations we define:

$$\langle \Gamma \rangle = \{(R, \tau) \mid (R, \tau) \text{ multi-sorted gadget- reduces to } \Gamma\}$$

Now we can state our multi-sorted Geiger theorem:

Theorem 11. *Fix $[t]$ and $\{D_b\}_{b \in [t]}$, and let Γ, Γ' be (possibly infinite) sets of multi-sorted relations and let $\mathcal{F}, \mathcal{F}'$ be (possibly infinite) sets of multi-sorted aggregators. Then*

1. $\mathrm{MInv}(\mathrm{MPol}(\Gamma)) = \langle \Gamma \rangle$

2. $\Gamma \subseteq \Gamma' \implies \mathrm{MPol}(\Gamma') \subseteq \mathrm{MPol}(\Gamma)$

3. $\mathcal{F} \subseteq \mathcal{F}' \implies \mathrm{MInv}(\mathcal{F}') \subseteq \mathrm{MInv}(\mathcal{F})$

Proof. Let us first recall the single-sorted Geiger theorem:

Theorem 12 (D. Geiger [Gei68])**.** *Fix D, and let Γ, Γ' be (possibly infinite) sets of relations on D and let $\mathcal{F}, \mathcal{F}'$ be (possibly infinite) sets of functions, such that each function is from some D power to D (i.e. aggregator functions for D). Then*

1. $\mathrm{Inv}(\mathrm{Pol}(\Gamma)) = \langle \Gamma \rangle$

2. $\mathrm{Pol}(\mathrm{Inv}(\mathcal{F})) = [\mathcal{F}]$

3. $\Gamma \subseteq \Gamma' \implies \mathrm{Pol}(\Gamma') \subseteq \mathrm{Pol}(\Gamma)$

4. $\mathcal{F} \subseteq \mathcal{F}' \implies \mathrm{Inv}(\mathcal{F}') \subseteq \mathrm{Inv}(\mathcal{F})$

In order to make the translation of our multi-sorted version to the above single-sorted one we first define

$$D = D_1 \dot{\cup} D_2 \dot{\cup} \cdots \dot{\cup} D_t$$

where D_b is the range for type b. If originally the D_bs are not disjoint, we make them disjoint without the loss of generality. A non-empty multi-sorted relation $X \subseteq D_{\tau_1} \times \cdots \times D_{\tau_m}$ can be now interpreted as the single-sorted relation $X_D \subseteq D^m$. We remark that viewing them as sets, X and X_D are exactly the same. The index D in X_D is only a reminder that we view X_D as a single sorted relation over domain D, while we view X as (X, τ). Since the D_bs are disjoint, from any such $X_D \neq \emptyset$ we can recover the types of every coordinate (the components of a single element of X_D already give this information). If Γ is a set of multi-sorted relations over a fixed type-set $[t]$, let Γ_D be the set of those X_Ds that $X \in \Gamma$.

For $b \in [t]$ we introduce the unary relation T_b on D (in the single sorted world):

$$T_b(u) \longleftrightarrow u \in D_b$$

In other words, $T_b(u)$ expresses that "u has type b in the multi-sorted world." For the set $\{T_1, \ldots, T_t\}$ of relations we introduce the notation Θ.

Definition 11. Let Δ be any set of relations on D such that $\Theta \subseteq \Delta$. Then for any polymorphism $f : D^n \to D$ of Δ and any $b \in [t]$ we can define $f_b : D_b^n \to D_b$ as $f_b(x) = f(x)$ on D_b^n.

Note. We know that f on D_b^n takes value from D_b since it is an aggregator of $T_b \in \Delta$.

We have now:

Lemma 13. *Let Γ be any set of multi-sorted relations over a fixed type-set $[t]$ and with the notations as before. Then the following are equivalent:*

1. *$(f_1, \ldots, f_t)$ is a multi-sorted polymorphism for Γ;*

2. *the sequence $f_1, \ldots, f_t$ arises, as in Definition 11, from some polymorphism f of $\Delta = \Gamma_D \cup \Theta$.*

We do not prove this easy lemma. Returning to the proof of Theorem 11, the only challenge is to prove 1. since 2. and 3. are obvious. It is also follows from known composition lemmas (polymorphisms compose, as do gadgets) that

$$\mathrm{MInv}(\mathrm{MPol}(\Gamma)) \supseteq \langle \Gamma \rangle$$

We have to show the containment in the other direction. Theorem 12 gives that

$$\mathrm{Inv}(\mathrm{Pol}(\Gamma_D \cup \Theta)) = \langle \Gamma_D \cup \Theta \rangle_D$$

Here the subscript in $\langle \cdot \rangle_D$ refers to that gadget generation is taken in the single sorted world. Our proof scheme is to relate $\langle \Gamma \rangle$ to $\langle \Gamma_D \cup \Theta \rangle_D$ and $\mathrm{MInv}(\mathrm{MPol}(\Gamma))$ to $\mathrm{Inv}(\mathrm{Pol}(\Gamma_D \cup \Theta))$.

Which non-empty relations can we generate from $\Gamma_D \cup \Theta$, i.e. what are the elements of $\langle \Gamma_D \cup \Theta \rangle$? A gadget with this set of generators is of the form

$$R(x_1, \ldots, x_k) = \exists y_1, \ldots, y_{k'} : R_1(z_{1,1}, \ldots, z_{1,k_1}) \wedge \ldots \wedge R_p(z_{p,1}, \ldots, z_{p,k_p}) \tag{1}$$

where each R_i is either from Γ_D or from Θ or the $=$ relation.

Definition 12. We say that (an x- or y-) variable z in (1) has type b if whenever the conjunct holds for an assignment (without the existential quantifier), z has a value in D_b. In different words, adding $T_b(z)$ to the conjunction would not eliminate any of the satisfying assignments of the conjunct.

Since a $\Gamma_D \cup \Theta$ gadget (recall, this is a single-sorted gadget) has variables only over D, there is no a priori type restriction (other than the entire D) on any variable. Nevertheless, if a variable z is involved in a relation S_D, where S is a relation from Γ, then S gives a type b to that variable: S_D never holds if $z \notin D_b$, so we might as well restrict z to D_b. Assume now that there is a variable z' such that the right hand side of (1) contains the relation $z = z'$ with an already restricted z. Then z' must also be from D_b. Of course, a chain of such equations also enforces a type on the variable in the end of the chain. Finally, any relation $T_b(z)$ enforces a type b on z. In summary, we can assign type b to variable z if

1. $T_b(z)$ occurs in the gadget;

2. z occurs in a constraint from Γ_D with type b;

3. There is a chain of equality relations that starts form any variable restricted to type b (by 1. or 2.) that leads to z.

We note that a variable cannot have two different (i.e. contradicting) types defined this way. Any contradiction in types would make R unsatisfiable (i.e. the empty relation). Therefore R is equivalent to a direct product of a "typed part" and an "untyped part":

$$R = R_{\mathrm{typed}} \times \underbrace{(w_{1,1} = \cdots = w_{1,s_1}) \times \cdots \times (w_{l,1} = \cdots = w_{l,s_l})}_{\text{untyped part}}$$

The $w_{i,j}$s are variables and the untyped (or typed) part might not be there. Point 1.-3. also give that R_{typed} is a syntactically recognizable part of R that arises by deleting some variables and terms from the right hand side. Although R_{typed} is a Γ_D-gadget (recall that Γ_D is an *untyped* set of relations

constructed from the *typed* set of relations, Γ), because of its syntax we can also read it as a (typed) Γ-gadget, and in addition with the exact same semantics (meaning that R_{typed} as a set is the exact same set as when we read the formula as a Γ-gadget). So R_{typed} [viewed as a multi-sorted relation] $\in \langle \Gamma \rangle$.

Next we claim that

$$R \in \text{MInv}(\text{MPol}(\Gamma)) \quad \longrightarrow \quad R_D \in \text{Inv}(\text{Pol}(\Gamma_D \cup \Theta)).$$

The left hand side reads that R is kept by all multi-sorted polymorphism $(f_1, ..., f_t) \in \text{MPol}(\Gamma)$. By Lemma 13 we have that $f \in \text{Pol}(\Gamma_D \cup \Theta)$ if and only if its component-sequence (as in Definition 11) $(f_1, ..., f_t) \in \text{MPol}(\Gamma)$. So R_D is kept by all $f \in \text{Pol}(\Gamma_D \cup \Theta)$, proving our claim.

By the single sorted Geiger theorem (applied to $\Gamma_D \cup \Theta$) we have then that since $R_D \in \text{Inv}(\text{Pol}(\Gamma_D \cup \Theta))$, we also have that $R_D \in \langle \Gamma_D \cup \Theta \rangle$. Two paragraphs earlier we have seen, that then R_D must be of the form $R_{\text{typed}} \times (\alpha_{1,1} = \cdots = \alpha_{1,s_1}) \times \cdots \times (\alpha_{l,1} = \cdots = \alpha_{l,s_l})$. But since all component of R_D are typed, only the typed part is there ($R_D = R_{\text{typed}} = R$ as sets). So $R \in \langle \Gamma \rangle$. $\qquad \square$

5 Gadgets characterize Impossibility

The Galois connection of Geiger (and its multi-sorted version) sends the message that the more gadgets we can create from a set of relations (or from a single relation), the smaller set of aggregators this set of relations has. An impossibility domain X does not have any non-trivial aggregator, therefore X is expected to generate all relations. Of corse, what excites us more is the converse. If we can write all relations as gadgets made from X and some simple relations then X must be an impossibility domain. There is however some work ahead:

1. We need to understand the role of the Idempotency (Supportiveness) conditions.

2. We want to find a minimal (for algorithmic reasons, but also for convenience) gadget set that already implies the impossibility of X.

5.1 The Idempotency and Supportiveness conditions

The Idempotency and Supportiveness conditions correspond to adding extra relations to our base set of relations from which we build the gadgets that prove the impossibility of X. Our base set is originally $\{X\}$. For the Idempotency condition we add all *Assignment-giving relations* and for the Supportiveness condition we add all *Unary relations* (notions defined below).

Definition 13 (Unary relations, $X^{\mho}$). A multi-sorted unary relation is $(x \in A, (a))$, where $a \in [t]$ is a type and $A \subseteq D_a$. For a multi-sorted relation X we define $X^{\mho}$ as the set of relations that consists of X and all unary relations for the type set $[t]$, $\{D_b\}_{b \in [t]}$ on which X is defined.

Definition 14 (Assignment-giving relations, X^+). Multi-sorted assignment-giving relations are unary relations of the form $(x = v, (a))$, where $v \in D_a$ (i.e. $|A| = 1$). X^+ is the set of relations that includes X and all assignment giving relations for the type set $[t]$, $\{D_b\}_{b \in [t]}$ on which X is defined.

Lemma 14. *A multi-sorted function $g = (g_1, \ldots, g_t)$, where $g_a : D_a^n \to D_a$, is idempotent, (meaning each g_a is idempotent) if and only if it aggregates all assignment giving relations for all types. It is supportive, if and only if it aggregates all unary relations for all types.*

We omit the simple proof of this known statement.

5.2 The Translation of the original problem

Before characterizing it with gadgets, we devote a short section to the exact notion of 'impossibility' in the algebraic language.

Lemma 15. *The following voting theory and algebraic conditions are equivalent:*

Algebra	Voting Theory
$X \subseteq D^m$ is a relation	$X \subseteq D^m$ is a Domain
$f = (f_1, \ldots, f_m)$, where $f_j : D_j^n \to D_j$. Here $D_j = \mathrm{pr}_j X$ by definition (resticting D to D_j is important).	IIA aggregator function $f : X^n \to X$
$\exists\, 1 \le k \le n :$ all f_j are projections on their k^{th} coordinate.	f is a Dictatorship
All f_js are idempotent (supportive)	f is idempotent (supportive)

The following voting theory and algebraic problems are equivalent:

Algebra	Voting Theory
Determine if X has idempotent (supportive) non-dictatorial multi-sorted polymorphism.	*Determine if X has idempotent (supportive) non-dictatorial IIA aggregator.*

X is an impossibility domain *if the answer to the above question is "No."*

5.3 Characterization of Impossibility Domains in terms of gadgets

Applying Lemmas 14, 15 and our multi-sorted Geiger's theorem (Theorem 11) it is not hard to show:

Lemma 16. *Domain $X \subseteq D^m$ is impossible with respect to IIA + Idempotency (Supportiveness) + Non-dictatorship if and only if* all *multi-sorted relations can be generated as multi-sorted X^+ ($X^{\mho}$) -gadgets. Here $t = m$, $D_j = \mathrm{pr}_j X$ for $1 \le j \le m$ and the typing of X is $(X, (1, \ldots, m))$.*

The set of all (multi-sorted) relations is however infinitely large! Luckily, we can select a finite subset (actually, in many different ways) that generate all relations, and it is sufficient to consider only those.

Definition 15 (The Non-Binary OR relation). We define the multi-sorted relation $R_{k,\ell}^{u,v}$ which is unsatisfied only when $x = u$ and $y = v$ simultaneously hold (x has type k and v has type ℓ). In formula:
$$R_{k,\ell}^{u,v}(x, y) = (\neg(x = u \wedge y = v), (k, \ell)).$$

Definition 16 (The multi-sorted Not-All-Equal relation). The multi-sorted NAE relation on types a, b, c is defined only when $D_a = D_b = D_c = \{0, 1\}$. In this case
$$\mathrm{NAE}_{a,b,c}(x, y, z) = (|\{x, y, z\}| > 1, (a, b, c)).$$

We are now ready to state our gadget-characterization of impossibility domains X:

Theorem 17. *Let $X \subseteq D^m$ non-degenerate. Let $t = m$ and $\tau = (1, \ldots, m)$, and the range for type j be $D_j = \mathrm{pr}_j X$. Then X is an impossibility domain with respect to IIA + Idempotency + Non-dictatorship if and only if there are $(X, \tau)^+$-gadgets expressing $R_{k,\ell}^{u,v}$ for every $1 \le k, \ell \le m$; $u \in \mathrm{pr}_k X$, $v \in \mathrm{pr}_\ell X$. Furthermore, if $|D_j| = 2$ for some $1 \le j \le m$, we also need to add the multi-sorted NAE gadget on types (j, j, j). The analogous statement, when we replace "Idempotency" with "Supportiveness" requires to replace $(X, \tau)^+$ with $(X, \tau)^{\mho}$.*

6 Gadget-power

First we give a proof of Theorem 17. We show the non-trivial direction, i.e. that if we can create all gadgets required by Theorem 17, the only polymorphisms that remain are dictatorships.

Remark 2. Even a single gadget present in $\langle \Gamma \rangle$ can have strong consequences. For instance, if we can construct the equality gadget $(x = y, (a, b))$ between two different types a and b (with a common alphabet), any multi-sorted polymorphism $(f_1, \ldots, f_t) \in \mathrm{MPol}(\Gamma)$ must have the same a and b components. We prove this in the end of the section.

Our way to prove Theorem 17 is to start to create gadgets and use them as "subroutines" to create even more gadgets. The following lemma says that for any fixed $1 \le k, \ell < t$ from $R_{k,\ell}^{u,v} \in \langle \Gamma \rangle$ one can construct *all* multi-sorted binary relation with type (k, ℓ) in $\langle \Gamma \rangle$.

Lemma 18. *Let $1 \le k, \ell \le t$ and $(S, (k, \ell))$ be any multi-sorted relation contained in $\mathrm{pr}_k X \times \mathrm{pr}_\ell X$. Then $(S, (k, \ell)) = \wedge_{(u,v) \notin S} R_{k,\ell}^{u,v}$.*

We omit the straightforward proof. Note that nothing stops us setting $k = \ell$ in the lemma, in which case we get all binary relations $(R \subseteq D_k^2)$. What does the presence of these relations in $\langle \Gamma \rangle$ say about the (multi-sorted) polymorphisms for Γ? They say a lot. In fact, if D_k has size at least three, already the not-equal relation, $(x \ne y, (k, k))$, alone excludes all idempotent (and so all supportive) polymorphisms other than the dictatorships *for that type*:

Lemma 19 (Not-equal gadget lemma)**.** *Assume that $((x \ne y), (k, k)) \in \langle \Gamma \rangle$. Then for every $f = (f_1, \cdots, f_t) \in \mathrm{MPol}(\Gamma)$ it must hold that f_k is a dictatorship on $\mathrm{pr}_k X$.*

The above lemma together with Lemma 18 imply

Lemma 20. *Assume that $|\mathrm{pr}_k X| \ge 3$ and the conditions of Theorem 17 hold, so we can create all $R_{k,\ell}^{u,v}$ from $(X, \tau)^+$ (resp. from $X, \tau)^\mho$). Then the kth component of any idempotent (supportive) aggregator $f = (f_1, \cdots, f_t)$ of X must be a dictatorship.*

What if $|\mathrm{pr}_k X| = 2$? Then the NAE gadget can be used to take care of the same thing.

Lemma 21 (Not-all-equal gadget lemma)**.** *Assume that the multi-sorted not-all-equal relation $(|x, y, z| > 1 \ \wedge \ x, y, z \in \mathrm{pr}_k X, (k, k, k))$ gadget-reduces to a set Γ of multi-sorted relations. Then for every $f = (f_1, \cdots, f_t) \in \mathrm{MPol}(\Gamma)$ it must hold that f_k is a dictatorship on $\mathrm{pr}_k X$.*

Among the conditions of Theorem 17 one explicitly states that in the case when $|\mathrm{pr}_k X| = 2$ the $(|x, y, z| > 1 \ \wedge \ x, y, z \in \mathrm{pr}_k X, (k, k, k))$ gadget can be constructed from $(X, \tau)^+$ (resp. from $X, \tau)^\mho$) to make Lemma 21 applicable.

Putting Lemmas 20 and 21 together, we conclude that if the gadgets promised by Theorem 17 are all present, then all components of every multi-sorted polymorphism $(f_1, \ldots, f_m)$ are dictatorships on the respective $\mathrm{pr}_j X$s.

To finish the "if" part of Theorem 17 all we need to show is that these dictatorships are controlled by the same index K (the dictator). Assume this is not the case, and let k and ℓ be components such that f_k is dictated by the Kth voter and f_ℓ is dictated by voter $L \ne K$. Because X is non-degenerate (and so $\mathrm{pr}_k X$ and $\mathrm{pr}_\ell X$ have size at least two) and because of König's theorem (or simply by basic combinatorics) there ought to be $u, v \in \mathrm{pr}_k X$ and $u', v' \in \mathrm{pr}_\ell X$ such that

1. $u \ne v$ and $u' \ne v'$;

2. There is an element U of X that takes u on k and u' on ℓ;

3. There is an element V of X that takes v on k and v' on ℓ.

Let us now aggregate a set of votes, all from $\{U, V\}$, but the Kth vote is U and the Lth vote is V. Then $(f_1, \ldots, f_m)$ aggregates this input to Z such that the kth issue aggregates to u and the ℓth issue aggregates to v'. Notice now that $R_{k,\ell}^{u,v'}$ holds for U and V, but not for Z, which is a contradiction, since every aggregator must keep all gadgets constructible from X^+ ($X^{\mho}$), in particular $R_{k,\ell}^{u,v'}$. This concludes the "if" (non-trivial) part of the proof of Theorem 17.

In the rest of the section we assume that for two types $a, b \in [t]$ we have $D_a = D_b$ (equivalently, a 1-1 correspondence '=' between D_a, D_b). We show that the ability to construct the '=' gadget between types a and b from a set Γ of (multi-sorted) relations implies that for every polymorphism $(f_1, \ldots, f_t)$ of Γ we have $f_a = f_b$. This can be useful, because the algebraic theory is developed mainly for single-sorted polymorphisms.

Lemma 22 (Equality gadget lemma). *Let Γ be a set of multi-sorted relations with type set $[t]$. Assume that for types a and b we have $D_a = D_b$, and that the multi-sorted equality relation $(x = y, (a, b))$ gadget-reduces to Γ. Then for every $f = (f_1, \cdots, f_t) \in \text{MPol}(\Gamma)$ it must hold that f_a is identical to f_b.*

Proof. We need to prove that for every $u = (u^1, \ldots, u^n) \in D_a^n$ ($= D_b^n$) it holds that $f_a(u) = f_b(u)$. Consider an arbitrary $u \in D_a^n$. f is a multi-sorted polymorphism of $(x = y, (a, b))$. This follows from the facts that $f = (f_1, \cdots, f_t)$ is a polymorphism of Γ and that $(x = y, (a, b))$ gadget-reduces to Γ. Therefore, since each line of the table

$$
\begin{array}{ccc}
\text{type } a & & \text{type } b \\
\\
u_1 & = & u_1 \\
u_2 & = & u_2 \\
& \vdots & \\
u_n & = & u_n \\
\hline
f_a(u) & = & f_b(u)
\end{array}
$$

above the solid horizontal line satisfies the $(x = y, (a, b))$ relation, we can apply polymorphism f for the two columns of the table. Now, as discussed, f must keep the relation $(x = y, (a, b))$, so $f_a(u) = f_b(u)$. $\qquad\square$

7 Example: Arrow's Theorem

Let $\mathcal{A} = \{A_1, \ldots, A_k\}$ denote a set of k items and let S_k be the domain that corresponds to the set of $k!$ different linear orders on $\mathcal{A}$ in a way we describe below. Each voter must vote for some linear order and the votes have to be aggregated into a single linear order, the "choice of the society."

Instead of thinking of a linear order as is (like $A_2 < A_3 < A_4 < A_1$) we rather represent it as a sequence of $\binom{k}{2}$ binary positions corresponding to questions of the form

$$A_1 < A_2? \,,\ A_1 < A_3? \,,\ \ldots \,,\ A_{n-1} < A_n?$$

(see also Section 2). When '$<$' is a linear order on $\mathcal{A}$, the answers to these questions ($0 = $ no; $1 = $ yes) uniquely (and even redundantly) encodes '$<$' in the form of a valid *evaluation*. The set of all

valid evaluations (these are binary vectors of length $\binom{n}{2}$) is exactly the relation $S_k \subseteq \{0,1\}^{\binom{n}{2}}$. Arrow famously shows:

Theorem 23 (Arrow [Arr50]). *When $k \geq 3$, there is no aggregator $f : S_k^n \to S_k$ for any $n \geq 2$ that satisfies IIA + Idempotency + Non-dictatorship.*

It is easy to see that the impossibility of S_3 implies the impossibility of S_k for $k \geq 3$. Below we are going to prove Theorem 23 when $k = 3$, using our method of gadgets. In the $A_1 < A_2$? $A_2 < A_3$? $A_3 < A_1$? basis (replacing '$A_1 < A_3$?' with '$A_3 < A_1$?' does not change the problem) we have that:

$$S_3 = \{001, 010, 011, 100, 101, 110\} = \text{NAE} \quad \text{(Not All Equal)}$$

Since Arrow allows to aggregate different coordinates with different aggregators, we view S_3 as a multi-sorted relation with type-set [3]. We need to show that the only polymorphisms of the multi-sorted relation set S_3^+ are projections (dictatorships). In section 3 we have created a gadget for the relation $(\neg(x = y), (1,3))$. Let us denote it by R_{13}. By symmetry, S_3^+-gadgets also exist for $R_{12} = (\neg(x = y), (1,2))$ and $R_{23} = (\neg(x = y), (2,3))$. Then the gadget

$$\exists x_2 : R_{12}(x_1, x_2) \wedge R_{23}(x_2, x_3)$$

expresses $(x_1 = x_3, (1,3))$ (see Fig. 2). We can similarly express any $(x_a = x_b, (a,b))$ for $1 \leq a < b \leq 3$. Once we have generated these relations, by Lemma 22 we conclude that every multi-sorted polymorphism of S_3^+ must be a single sorted polymorphism i.e. of the form (f_1, f_1, f_1), and it is well known that all single-sorted idempotent polymorphisms of NAE are dictatorships.
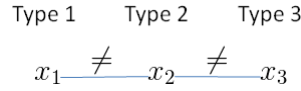

Figure 2: The gadget expressing $x_1 = x_3$.

8 Example: Pairwise distinctness

We continue to illustrate how one can use hand-made gadgets to prove impossibility theorems for specific domains:

Theorem 24. *Let D and m such that $|D| > m = 2$ or $|D| = m \geq 3$. Define*

$$X = \{(x_1, \ldots, x_m) \in D^m \mid x_1, \ldots, x_m \text{ are pairwise distinct}\}$$

Then X is an impossibility domain with respect to IIA + Idempotency + Non-dictatorship conditions.

In [DH10b], this theorem is proven under the IIA + Supportiveness + Non-dictatorship conditions. A special case of this theorem, i.e. when $|D| = m \geq 3$, can be derived from results in [FF11]. We give a gadget proof for it when $m = 2$ and $|D| = 3$, which is in a sense the hardest setting of the parameters. In this case the relation $X \subseteq [3]^2$ is a binary relation of type $(1,2)$, and we have to show that $\text{MPol}(X^+)$ contains only projections (dictatorships).

We remark that the problem in this case is essentially equivalent to showing that three coloring of bipartite graphs is NP-hard as long as assignment giving constraints are also allowed, i.e. we are

allowed to declare that "vertex v has color c". If we drop the bipartite condition, then the problem is well-known to be NP hard. The bipartite condition comes from the multi-sorted nature of the problem: relation X can connect only type 1 variables with type 2 variables.

First we create a gadget for the relation $(\neg(x_1 = x_2 = 2), (1,1))$. Clearly, by symmetry, then gadgets also exist for any $(\neg(x = y = a), (b,b))$, where $1 \leq a \leq 3$ and $1 \leq b \leq 2$.
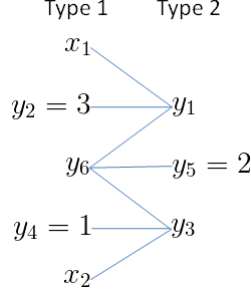
Type 1   Type 2

x_1

$y_2 = 3 \longrightarrow y_1$

$y_6 \longleftarrow y_5 = 2$

$y_4 = 1 \longrightarrow y_3$

x_2

Figure 3: The inequality gadget

The gadget that achieves this (see Fig. 3) corresponds to the following formula:

$$
\begin{aligned}
R(x_1, x_2) \quad = \quad & \exists y_1, \ldots, y_6 : \; X(x_1, y_1) \wedge X(x_2, y_3) \wedge X(y_2, y_1) \wedge X(y_4, y_3) \wedge X(y_6, y_1) \wedge \\
& \wedge X(y_6, y_3) \wedge X(y_6, y_5) \wedge (y_2 = 3) \wedge (y_4 = 1) \wedge (y_5 = 2)
\end{aligned}
$$

It is not hard to check that R implements the $(\neg(x_1 = x_2 = 2), (1,1))$ relation. Let us now denote the relation $(\neg(x = y = a), (b,b))$ by R_a^b. Then $R_1^b(x,y) \wedge R_2^b(x,y) \wedge R_3^b(x,y)$ expresses the $(x \neq y, (b,b))$ relation. Finally, the gadget

$$
T(x_1, x_2) = \exists y_1, y_2 : \; (x_1 \neq y_1) \wedge (x_1 \neq y_2) \wedge (y_1 \neq y_2) \wedge X(y_1, x_2) \wedge X(y_2, x_2)
$$

expresses $(x_1 = x_2, (1,2))$ (see Fig. 4). Once we have generated this relation, by lemma 22 we conclude that every multi-sorted polymorphism of X^+ must be a single sorted polymorphism i.e. of the form (f_1, f_1). It is well known that the only idempotent polymorphisms of the $x \neq y$ (single-sorted) relation are the dictatorships.

Type 1   Type 2

y_1

$\neq \quad \neq$

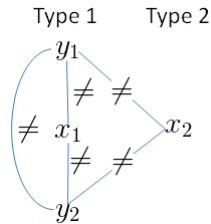$\neq \quad x_1 \qquad x_2$

$\neq \quad \neq$

y_2

Figure 4: The equality gadget

9   Binary Evaluations

In this section we first translate the total blockades condition to the algebraic language, then using it revisit the case of binary evaluation giving an alternative proof to the classification Theorem of E. Dokow, R. Holzman, and also indicate the proof of Theorem 10.

9.1 Total blockedness and its consequences

Lemma 25. *Let $X \subseteq \{0,1\}^m$ be totally blocked (see Definition 4) and non-degenerate. Let (X, τ) be any typing of the variables of X from a type-set $[t]$, $D_a = \{0,1\}$ for $1 \le a \le t$. We also assume that all types are used. Then for all $1 \le a, b \le t$: $(x = y, (a, b))$ (multi-sorted) gadget-reduces to X^+.*

Proof. Recall that the total blockedness condition means that on the vertex set $V = [m] \times \{0,1\}$ we have a strongly connected graph defined as follows: There is a directed edge from $(k, \epsilon) \in V$ to $(\ell, \epsilon') \in V$ where $k \ne \ell$ if and only if there are: (i.) a subset $S \subseteq [m]$ such that $k, \ell \in S$ and (ii.) a (partial-)evaluation $u : S \to \{0,1\}$ with $u_k = \epsilon$ and $u_\ell = 1 - \epsilon'$ such that there is no extension of u to any full evaluation x in X, but if we flip any bit of u then the resulting partial evaluation extends to some element of X. Let us focus on a directed edge $((k, \epsilon), (\ell, \epsilon'))$ as above, with $S = \{k, \ell, s_1, \ldots, s_q\}$ (we fix this S for $k, \ell, \epsilon, \epsilon'$), and create the gadget

$$E_{k,\ell,\epsilon,\epsilon'}(x_k, x_\ell) = \exists y_{s_1}, \ldots, y_{s_q}, \vec{y}: \ X(x_k, x_\ell, y_{s_1}, \ldots, y_{s_q}, \vec{y}) \wedge (y_{s_1} = u_{s_1}) \wedge \ldots \wedge (y_{s_q} = u_{s_q})$$

Here with some abuse of the notation we tried to indicate, via the indices, the variables' positions in X. In particular, $\vec{y}$ collects the $m - 2 - q$ variables of X that are not in $S = \{k, \ell, s_1, \ldots, s_q\}$. We remark that the type of a variable is uniquely determined by its position in X. Then we have

$$E_{k,\ell,\epsilon,\epsilon'}(\epsilon, \epsilon') = 1, \quad E_{k,\ell,\epsilon,\epsilon'}(\epsilon, 1 - \epsilon') = 0, \quad E_{k,\ell,\epsilon,\epsilon'}(1 - \epsilon, 1 - \epsilon') = 1$$

All three equations follow from the fact that $u : S \to \{0,1\}$ with $u_k = \epsilon$ and $u_\ell = 1 - \epsilon'$ was a minimally unsatisfying partial assignment, thus if we change the value of exactly one of the u_k, u_ℓ, the assignment becomes satisfying. Consider now a chain

$$((k^0, \epsilon^0), (k^1, \epsilon^1)), \ ((k^1, \epsilon^1), (k^2, \epsilon^2)), \ \ldots, ((k^{t-1}, \epsilon^{t-1}), (k^t, \epsilon^t))$$

of edges in the blockedness graph, for which we have generated relations $E_{k^0, k^1, \epsilon^0, \epsilon^1}, \ldots, E_{k^{t-1}, k^t, \epsilon^{t-1}, \epsilon^t}$ as above. Create the gadget

$$R(x_{k^0}, x_{k^t}) = \exists y_{k^1}, \ldots, y_{k^{t-1}}: \ E_{k^0, k^1, \epsilon^0, \epsilon^1}(x_{k^0}, y_{k^1}) \wedge \ldots \wedge E_{k^{t-1}, k^t, \epsilon^{t-1}, \epsilon^t}(y_{k^{t-1}}, x_{k^t})$$

It is easy to see that the typing is consistent. If we set $x_{k^0} = \epsilon^0$ then inductively all y_{k_i} variables are forced to take ϵ^i, eventually forcing $x_{k^t} = \epsilon^t$. On the other hand $R(1 - \epsilon^0, 1 - \epsilon^t) = 1$. To show this it is sufficient to set all y_{k_i} variables to $1 - \epsilon^i$ in the right hand side of the above formula. Since the blockedness graph is strongly connected, for any $a, b \in [t]$ with $\text{type}(x_k) = a$, $\text{type}(x_\ell) = b$ for some $1 \le k, \ell \le m$ and for any $\epsilon_k, \epsilon_\ell \in \{0,1\}$ we can build now gadget $R_{a,b,\epsilon,\epsilon'}$ that forces $x_\ell = \epsilon_\ell$ as long as $x_k = \epsilon_k$ and also permits the $x_k = 1 - \epsilon_k$, $x_\ell = 1 - \epsilon_\ell$ assignment, and a gadget $R'_{a,b,1-\epsilon,1-\epsilon'}$ that forces $x_\ell = 1 - \epsilon_\ell$ as long as $x_k = 1 - \epsilon_k$ and also permits the $x_k = \epsilon_k$, $x_\ell = \epsilon_\ell$ assignment. Then $R_{a,b,\epsilon,\epsilon'} \wedge R'_{a,b,1-\epsilon,1-\epsilon'}$ implements $x_k + \epsilon_k = x_\ell + \epsilon_\ell \mod 2$. In particular, by choosing $\epsilon k = \epsilon \ell = 0$ we have implemented the $(x = y, (a, b))$ relation. $\qquad \square$

Example 2. Let $X = \{000, 011, 101, 110\} = \{xyz \in \{0,1\}^3 \mid x + y + z = 0 \mod 2\}$. We also assume that $[t] = 3$ and the ith coordinate has type i. Then the minimally infeasible partial evaluations (MIPEs) are all those $xyz \in \{0,1\}^3$ for which $x + y + z = 1 \mod 2$. Then the blockedness graph is the directed complete graph (i.e. directed edges are drawn both ways for every edge). For $k = 1$, $\ell = 2$, $\epsilon_k = 0, \epsilon_\ell = 1$ we can create the gadget (based on $S = \{1, 2, 3\}$, $u = 001$):

$$E_{1,2,0,1}(x_1, x_2) = \exists y: \ X(x_1, x_2, y) \wedge (y = 1)$$

This together with $E_{1,2,1,0}$ created from $S = \{1, 2, 3\}$, $u = 111$ (accidentally, the two gadgets turn out to be the same, so the conjunction remains $E_{1,2,0,1}(x_1, x_2)$) gives the $(x \ne y, (1, 2))$ relation, as one can check it directly.

Lemma 26. *Let $X \subseteq \{0,1\}^m$, totally blocked. Then every aggregator $f = (f_1, \ldots, f_m)$ which is IIA + Idempotent satisfies that all f_j's are identical.*

Proof. Let $t = m$ and view X as the multi-sorted relation $(X, (1, 2, \ldots, m))$. Then $(x = y, (k, \ell))$ $(1 \leq k, \ell \leq m)$ gadget-reduces to X^+ by Lemma 25. Since f is an idempotent IIA aggregator of X we have that $f \in \mathrm{MPol}(X^+)$. Combining the above two things the statement then follows from Lemma 22. □

We remark (although do not use it in the sequel) that total blockedness also generates all non-equal relations:

Lemma 27. *Let $X \subseteq \{0,1\}^m$, totally blocked. and X has type $(X, (1, \ldots, m))$. Then X (as a multi-sorted relations) generates all relations of the form $(x \neq y, (a, b))$, where $a, b \in [t]$.*

9.2 A new proof of Theorem 5

We give a new proof of the interesting part of Theorem 5 (E. Dokow, R. Holzman, [DH10a]), i.e. that when X is totally blocked, it is a possibility domain (with respect to IIA+Idempotency+No Dictatorship) if and only if it is an affine subspace. The new proof uses results from the algebraic theory of constraint satisfaction problems.

Lemma 26 gives that when X is totally blocked, all idempotent multi-sorted polymorphisms of X are single-sorted and we can use Schaefer's theorem, or more precisely algebraic version of it (Hubie Chen [Che09]) to determine the types of functions in $\mathrm{Pol}(X)$:

Theorem 28 (Schaefer, algebraic version). *Let $D = \{0,1\}$ and Γ be a set (single-sorted) relations on D. Then Γ^+ either has one of the following four operations as a polymorphism:*

1. *The binary AND operation $\wedge$;*

2. *The binary OR operation $\vee$;*

3. *The ternary majority operation $\mathrm{Maj}_3(x, y, z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$;*

4. *The Mal'tsev operation $u - v + w \mod 2$.*

Otherwise $\mathrm{Pol}(\Gamma^+)$ contains only projections (dictatorships).

Theorem 28 gives that when X is totally blocked and X is not an impossibility domain then one of the cases 1.-4. must hold. But [DH10a] proves more, it shows that when X is totally blocked, only Case 4. and the default case (i.e. no non-trivial polymorphisms) may occur. We provide a brief proof of this. We exclude Cases 1.-3. as follows:

Excluding 1. and 2: We show that if $\vee \in \mathrm{Pol}(X)$, then in the blockedness graph, no node of the form $(k, 1)$ has a directed edge to any node of the form $(\ell, 0)$, so the blockedness graph cannot be strongly (or anyhow) connected. For this it is sufficient to show that every MIPE has at most one variable set to 1. Suppose that $x_k = x_\ell = 1$ is part of a MIPE with $k \neq \ell$ and the rest of MIPE evaluates to α. By the definition we have assignments:

	x_k	x_ℓ	rest of MIPE	rest				
(	1	1	α	any	)	never $\in$	X	(since it is MIPE)
(	0	1	α	some	)	$\in$	X	(since it was MIPE)
(	1	0	α	some	)	$\in$	X	(since it was MIPE)
(	$0 \vee 1$	$1 \vee 0$	α	some	)	$\in$	X	(assgnm 2 $\vee$ assgnm 3)

Then the first and fourth lines of the table contradict to each other. An analogous proof shows that when $\wedge \in \mathrm{Pol}(X)$ the blockedness graph is not strongly connected.

Excluding 3: Assume that X is totally blocked and $\mathrm{Maj}_3 \in \mathrm{Pol}(X)$. First we show:

Lemma 29. *If* $\mathrm{Maj}_3 \in \mathrm{Pol}(X)$ *then every MIPE for X has length at most two.*

Proof. Consider a MIPE S, which contrary to our assumption has at least three elements, x_1, x_2, x_3. Assume that x_i evaluates to u_i for $1 \le i \le 3$, while the rest of the MIPE evaluates to α. Then the first and fifth lines of the following table together give a contradiction:

	x_1	x_2	x_3	rest of MIPE	rest				
(	u_1	u_2	u_3	α	any	)	never $\in$	X	(since it is MIPE)
(	$1 - u_1$	u_2	u_3	α	some	)	$\in$	X	(since it was MIPE)
(	u_1	$1 - u_2$	u_3	α	some	)	$\in$	X	(since it was MIPE)
(	u_1	u_2	$1 - u_3$	α	some	)	$\in$	X	(since it was MIPE)
(	u_1	u_2	u_3	α	some	)	$\in$	X	Maj_3(assgnms 2,3,4)

$\square$

Assume now that we have an edge from (k, ϵ) to (ℓ, ϵ') in the blockedness graph. Since the MIPE creating this edge, by Lemma 29 has length two (cannot have length one), we conclude that $x_k = \epsilon$ forces $x_\ell = \epsilon'$. Consider any $x \in X$, by our assumption the total blockedness graph is strongly connected so there is a path from $(1, x_1)$ to $(1, 1 - x_1)$, which in the light of the above argument means that $(1, x_1)$ forces $(1, 1 - x_1)$ through a sequence of edges, which is an obvious contradiction. Thus X is empty.

Schaefer's theorem now tells us that X must be either an impossibility domain or an affine subspace. So what about the case when X is not totally blocked? Then we use the following deep theorem of A. Bulatov and P. Jeavons:

Theorem 30 (Bulatov and Jeavons [BJ03])**.** *Let $D = \{0, 1\}$ and Γ be a set of multi-sorted relations on D with type set $[t]$. Then for every type $j \in [t]$ either for every $\vec{f} = (f_1, \cdots, f_t) \in \mathrm{MPol}(\Gamma^+)$ the jth component is a dictatorship or there is an $\vec{f} = (f_1, \cdots, f_t) \in \mathrm{MPol}(\Gamma^+)$ such that f_j is one of*

1. *the semi-lattice operation $u \vee v$ or $u \wedge v$,*

2. *the majority operation $(u \vee v) \wedge (v \vee w) \wedge (w \vee u)$,*

3. *the Mal'tsev operation $u - v + w \mod 2$.*

From this Theorem 10 easily follows.

10 Non-binary Evaluations

In this section we complete the classification theorem of Dokow and Holzman [DH10b] for non-binary evaluations. While the two authors have only considered the supportive case, here we resolve the idempotent case as well.

10.1 General notion of total blockedness

Dokow and Holzman [DH10b] have developed the the notion of total blockedness in the non-binary case, i.e. for a general domain D. Our characterization theorems will use their notion.

Definition 17. Total blockedness for non-binary X is defined in [DH10b]. X is totally blocked if and only if the following directed graph on the vertex set

$$V = \{\sigma\sigma_j' |\quad j \in [m]\quad \wedge\quad \sigma, \sigma' \in \mathrm{pr}_j X\quad \wedge\quad \sigma \neq \sigma'\}$$

is strongly connected. There is an edge from $\sigma\sigma_k'$ to $\rho\rho_\ell'$ where $k \neq \ell$ if and only if there are

$$B_1 \subseteq \mathrm{pr}_1 X,\ B_2 \subseteq \mathrm{pr}_2 X,\ \ldots\ ,\ B_m \subseteq \mathrm{pr}_m X$$

such that

1. Each $|B_j| = 2$ $(1 \leq j \leq m)$;

2. $B_k = \{\sigma, \sigma'\}$ and $B_\ell = \{\rho, \rho'\}$;

3. Introduce the notation $X_B = X \cap \prod_{j=1}^m B_j$. Then X_B is a binary relation (think of each B_i as $\{0, 1\}$). Condition 3. is that under these definitions (k, σ) is connected with (ℓ, ρ) in the blockedness graph of X_B (see Definition 3 for the blockedness graphs for binary domains).

10.2   Supportive non-binary evaluations

First we restate *the supportive* part of Theorem 8:

Theorem 31. *Let $X \subseteq D^m$, non-degenerate and non-binary. If X is totally blocked then X is an impossibility domain with respect to IIA + Supportiveness + Non-dictatorship if and only if X is an impossibility domain with respect to IIA + Supportiveness + Non-dictatorship with the $n \leq 3$ condition (meaning that we find no other aggregators than dictatorships when we restrict ourselves to aggregators with only three arguments).*

Remark 3. The theorem is a classification theorem in the sense that it gives us an algorithm to determine if a given domain X is an impossibility domain with respect to IIA + Supportiveness + Non-dictatorship or not: just check all potential aggregators with at most three arguments.

Proof. The 'only if' part is straightforward since if X is an impossibility domain with respect to IIA + Supportiveness + Non-dictatorship then every supportive IIA aggregator $f = (f_1, \ldots, f_m)$ of X is a dictatorship, not only for arity $n \leq 3$. For the 'if' part we need the following results of E. Dokow and R. Holzman:

Definition 18 (E. Dokow and R. Holzman [DH10b])**.** Let $f = (f_1, \ldots, f_m)$ be a supportive IIA aggregator of arity n for $X \subseteq D^m$. For an issue j and an ordered pair of distinct positions $u, v \in D_j$ we translate $f_j|_{\{u,v\}} : \{u, v\}^n \to \{u, v\}$ to a function $W_j^{uv} : \{0, 1\}^n \to \{0, 1\}$ under $0 \leftrightarrow v,\ 1 \leftrightarrow u$.

Lemma 32 (E. Dokow and R. Holzman [DH10b], Propostion 1)**.** *If X is totally blocked, then all $W_j^{uv}s$ are the same.*

Definition 19 (E. Dokow and R. Holzman [DH10b])**.** We call f *2-dictatorial* if all W_j^{uv}s $(j \in [m]$, $u, v \in D_j)$ are dictatorships with respect to the same k.

Lemma 33 (E. Dokow and R. Holzman [DH10b], Proposition 5)**.** *If X is totally blocked and f is 2-dictatorial then f is a dictatorship.*

Let us try to put the above two lemmas together! The total blockedness is a condition in the theorem whose 'if' part we want to prove, so what is missing is that under the theorem's conditions the W_j^{uv}s are not simply the same, but they are all dictatorships. We rely on the following lemma which is essentially a simplified version of Theorem 2.16 in [Bul11] and a multi-sorted version of Schaefer's dichotomy theorem (see Theorem 28 and [Che09]).

Lemma 34. *Let Γ be a set of multi-sorted relations over D with type set $[t]$. If Γ does not have IIA + Supportiveness + Non-dictatorship aggregators with the $n \leq 3$ condition, then for any $f = (f_1, \cdots, f_t) \in \mathrm{MPol}(\Gamma^{\mho})$, $a \in [t]$, $u, v \in D_a$ with $u \neq v$ the restriction $f_a|_{\{u,v\}}$ is a dictatorship.*

Proof. (of Lemma 34.) Assume the contrary, namely that Γ does not have IIA + Supportiveness + Non-dictatorship aggregators with $n \leq 3$, but it has some aggregator $f = (f_1, \cdots, f_t) \in \mathrm{MPol}(\Gamma^{\mho})$, such that there exist $a \in [t]$ and $u, v \in D_a$, $u \neq v$ with the property that $f_a|_{\{u,v\}}$ is not a dictatorship, where n is the arity of f. Then n must be at least 4. Let f be such a counter-example with minimal n. In particular, any $f' = f(x^{(1)}, \ldots, \underbrace{x^{(i)}}_{i^{\text{th}} \text{ argument}}, \ldots, \underbrace{x^{(i)}}_{i'^{\text{th}} \text{ argument}} \ldots, x^{(n)})$, i.e. when we identify two inputs, must be a two-dictatorship, because f' aggregates $n - 1$ inputs.

Denote $f_a|_{\{u,v\}}$ by g, which is presumably not a dictatorship. We will arrive at a contradiction by showing that g is a dictatorship, i.e. there exists one $k \in [n]$ such that for any $x_1, \cdots, x_n \in D'$, $g(x_1, \cdots, x_n) = x_k$. Since any identification of the variables of g arises by first identifying these variables in f, and then restricting the resulting type $= a$ component to the binary set $\{u, v\}$, we have, that any identification of variables of g, must result in a dictatorship. If <u>all</u> of these identifications $x^{(i)} = x^{(i')}$ result in a dictatorship that projects to coordinate i (as opposed to some coordinate $i'' \notin \{i, i'\}$), we get a contradiction by setting $\{i, i'\}$ first to $\{1, 2\}$ then to $\{3, 4\}$:

$$u = f(\underbrace{u, u}, v, v, \ldots) = f(u, u, \underbrace{v, v}, \ldots) = v. \quad (\text{Used that } n \geq 4.)$$

Thus there exist two coordinates where identifying the corresponding variables will result in a dictatorship function that projects to <u>some other</u> (i.e. not i, i') coordinate. Wlog assume that

$$g(\underbrace{x_1, x_1}, x_3, x_4, \cdots, x_n) = x_4$$

Then $g(x_1, x_1, x_1, x_4, \cdots, x_n) = x_4$. We show that this implies $g(x_1, x_2, x_1, x_4, \cdots, x_n) = x_4$. If $g|_{x_3=x_1}$ was a dictator x_i other than x_4, then setting $x_2 = x_1$ and letting x_4 vary we would get a contradiction. Similar reasoning gives that $g(x_1, x_3, x_3, x_4, \cdots, x_n) = x_4$. Thus whenever there is a duplication among the values of x_1, x_2, x_3, the output of g is always x_4. But duplication always occurs since $|D'| = 2$, thus g is a dictatorship, a contradiction. $\qquad\square$

We are now ready to prove the 'if' part of Theorem 31. Assume that when $n \leq 3$ there are no other supportive aggregators for X than dictatorships (and the other conditions: X is non-degenerate, totally blocked) also hold. Consider an aggregator f for X with $n \geq 4$. By Lemma 34, for any $j \subseteq [m]$ and for any $u, v \in D_j$, $u \neq v$, we have W_j^{uv} is a dictatorship. By Lemma 32, since X is totally blocked, all W_j^{uv} are the same. Lemma 33 then implies that f is a dictatorship. $\qquad\square$

10.3 General idempotent non-binary evaluations

Lemma 35. *For a given domain $X \subseteq D^m$, non-degenerate and non-binary, i.e. $|D| = d \geq 3$, and totally blocked, if X does not have any IIA + Idempotency + Non-dictatorship aggregator with $n \leq d$ condition, then X is an impossibility domain with respect to IIA + Idempotency + Non-dictatorship.*

Proof. Assume by contradiction that X satisfies the condition of the lemma and X is a possibility domain with respect to IIA + Idempotency + Non-dictatorship. Then there is an idempotent IIA aggregator $f = (f_1, \cdots, f_m)$ which is not a dictatorship. By the hypothesis of the lemma, f has arity

$n \geq d + 1$. Assume that f is of minimal arity, i.e. no idempotent non-dictatorial aggregator with smaller arity exists. We first show that f is supportive, i.e.

$$\forall\, x^{(1)}, \cdots, x^{(n)} \in X \qquad \forall\, 1 \leq j \leq m\ : \qquad f_j(x_j^{(1)}, \cdots, x_j^{(n)}) \in \{x_j^{(1)}, \cdots, x_j^{(n)}\}.$$

We are done if we can show that for any <u>fixed</u> $x^{(1)}, \cdots, x^{(n)}$ and j we have $f_j(x_j^{(1)}, \cdots, x_j^{(n)}) \in \{x_j^{(1)}, \cdots, x_j^{(n)}\}$. We use the pigeon hole principle. Since $n \geq d + 1$, among $x_j^{(1)}, \cdots, x_j^{(n)}$ there must be at least two elements which are the same. For notational conveniences they are $x_j^{(1)}$ and $x_j^{(2)}$.

Remark 4. The collision does not happen at the same pair of indices for all inputs and js, but this does not affect us, since we are setting the input fixed.

Since the collision is at indices 1 and 2, we are going to examine the aggregator of $n-1$ elements g that we get from f by identifying the first two inputs of f. Since g is also an idempotent IIA aggregator of X, by our minimality assumption g must be a dictatorship. Thus g_j is also a dictatorship and therefore supportive. In particular,

$$u = g_j(x_j^{(2)}, \cdots, x_j^{(n)}) \in \{x_j^{(2)}, \cdots, x_j^{(n)}\}.$$

But u is also the value that f_j takes on $x_j^{(1)}, x_j^{(2)} \cdots, x_j^{(n)}$ (since by our assumption $x_j^{(1)} = x_j^{(2)}$). This concludes the proof of the fact that f if supportive.

Then, since we have found a non-dictatorial supportive aggregator for X (on some number of inputs), by Theorem 31 there must also be a non-dictatorial supportive aggregator on three inputs. Since supportive aggregators are also idempotent we get into a contradiction with the Lemma's assumption that the smallest non-dictatorial idempotent aggregator is on more than $|D| \geq 3$ inputs. $\qquad\square$

This lemma resolves the *idempotent case*, which was the remaining part of Theorem 8.

11 Algorithms to determine impossibility

When we try to determine if $X \subseteq D^m$ is an impossibility domain or not with respect to IIA + Idempotency (or Supportiveness) + Non-dictatorship, we can rely on two different types of characterization theorems: By gadgets (Theorem 17); by aggregators (Theorem 8). Both types lead to algorithmic solutions, and we can use both of them as alternatives.

11.1 Algorithms from the characterization by gadgets

As we have seen in the previous sections, to determine if X is an impossibility domain with respect to IIA + Idempotency (or Supportiveness) + Non-dictatorship, we need to check if certain relations can be expressed as X^+-gadgets ($X^\mho$- gadgets). This is stated in Theorem 17. The task is therefore to solve the following type of problem:

Find Gadget: Given a set Γ of relations over D and a relation R over D determine if there is a Γ-gadget for R. In the multi-sorted version the relations are over a type set $[t]$ with associated domains $D_1, \ldots, D_t$.

At first a hurdle seems to be that the gadgets may contain arbitrary (un-specified) number of auxiliary variables. Due to Geiger [Gei68], Jeavons [Jea98] and Trevisan et. al. [TSSW96], we however know

that the number of auxiliary variables in the *smallest* Γ-gadget for R is upper bounded in terms of $|R|$, $|D|$ and $|\Gamma|$. The above results easily generalize to the multi-sorted case. In our setting $|\Gamma|$ is either X^+ or $X^{\mho}$. The sizes of the latter are upper bounded in terms of m and $|D|$. Unfortunately, straightforward implementations yield a double-exponential running time in $|X|$, D and m, and whether we can reduce it to single exponential, we currently do not know.

In spite of their large worst case computational times, gadgets often provide very economical witnesses to impossibility (see our two concrete earlier examples), and in all cases the witness size is at most exponential in the above parameters.

11.2 Algorithms from the characterization by aggregators

Theorem 8 gives us a complete classification of impossibility domains for abitrary (binary or non-binary) evaluations. Here we turn these into algorithms. We assume without loss of generality that X is non-degenerate.

Algorithm. Determines if $X \subseteq D^m$ is an impossibility domain under the IIA + Supportiveness + Non-dictatorship condition:

1. Check if X is totally blocked (see Definition 17). If X is not totally blocked, then X is a possibility domain.

   Otherwise:

2. FOR each supportive $f = (f_1, \ldots, f_m)$ where $f_j : D_j^3 \to D_j$, check if f aggregates X and it is a Non-dictatorship. If our search returns an f satisfying the criteria, then X is a possibility domain, otherwise it is an impossibility domain.

Note: it is enough to look only at $n = 3$ as opposed to $n \leq 3$. The running time is dominated by step 2. The number of fs in the search is upper bounded by $|D|^{m \cdot |D|^3}$. To check for dictatorship is trivial. To check if f is an aggregator of X takes $\text{poly}(|X|, m, |D|)$ time. Thus we have:

Theorem 36. *The complexity to determine if a given domain $X \subseteq D^m$ is an impossibility domain with respect to IIA + Supportiveness + Non-dictatorship is in $O(\text{poly}(|X|, m, |D|)|D|^{m \cdot |D|^3})$.*

Similarly (we must replace 3 with $|D|$) we get:

Theorem 37. *The complexity to determine if a given domain $X \subseteq D^m$ is an impossibility domain with respect to IIA + <u>Idempotency</u> + Non-dictatorship is in $O(\text{poly}(|X|, m, |D|) \cdot |D|^{m \cdot |D|^{|D|}})$.*

Note that we view D as constant (binary, etc.) and consequentially view the above complexities as single exponential.

12 Degrees of democracy

Although the Non-dictatorship condition represents minimal criterion for democracy, there are many functions that pass the Non-dictatorship test, but can barely be called democratic. Consider for instance the Boolean function that takes the majority value if the first voter votes zero, and takes the value one otherwise. Although this is not dictatorship the first voter has an overwhelming way in the outcome. What voting functions should we consider democratic? Scenarios taken from real life, such

as the American electoral system (iterated majority function), show that the majority vote is not the only one that can be viewed as truly democratic. The answer is non-trivial.

Different criteria for democracy have been formulated such as Anonymity (invariant under S_n) or Symmetricity, by Kalai [Kal02] (invariant under a transitive permutation group acting on $[n]$), that are somewhere on the scale in between the majoritarian and dictatorial voting schemes. In this article we would like to introduce StrongDem, with deep algebraic motivation.

StrongDem: Let f be an aggregator for $X \subseteq D^m$ for $n \geq 2$ voters that satisfies the IIA condition, so it is of the form $f = (f_1, \ldots, f_m)$. We say that f is StrongDem if for every $1 \leq j \leq m$, $1 \leq i \leq n$ there are $c_1, \ldots, c_n \in D_j$ such that $f_j(c_1, \ldots, c_{i-1}, x, c_{i+1}, \ldots, c_n)$ does not depend on $x \in D_j$. We further require that this property holds not only for D_j but when we replace D_j with any $D'_j \subseteq D_j$ such that the operation f preserves (respects) D'_j. (In the replacement the independence from x must hold only when x is also from D'_j.)

The majority function on three or more arguments is in StrongDem: take any $D' \subseteq D$ and set all votes except the vote of voter i on the jth issue to some (arbitrary) $c \in D'$. Then the outcome will be c no matter what position the ith voter takes. Since any StrongDem aggregator is clearly Non-dictatorship, we have the containment:

$$\text{Non-dictatorship} \ \supset \ \text{StrongDem} \ \supset \ \text{Majority voting}$$

All containments are strict in the following strong sense: For any two of the above conditions we can find X which is a possibility domain with respect to the larger class, but an impossibility domain for the smaller (IIA + Idempotency are assumed). An important example for an X which admits an f with the Non-dictatorship condition, but has no StrongDem voting scheme is the affine subspace. Let $D = \{0, 1\}$, and $X = \{(x_1, x_2, x_3) \in D^3 \mid x_1 + x_2 + x_3 = 1 \mod 2\}$. There is a non-dictatorial voting scheme when n is odd: Let $f_j : (u_1, \ldots, u_n) \rightarrow \sum_{i=1}^n u_i \mod 2$ for $1 \leq j \leq 3$. It is easy to see that $f = (f_1, f_2, f_3)$ has the Non-dictatorship property. It can be shown that this is the *only* type of non-dictatorial aggregator for X, and it is not StrongDem.

Majority, Anonymity, Symmetricity	The scheme treats all voters exactly in the same way
StrongDem	When all others votes are appropriately fixed, a single voter cannot change the outcome
Non-dictatorship	There is not a single voter who exclusively controls the outcome.

Figure 5: Conditions on democracy and their informal meaning

The StrongDem condition is equivalent to the aggregator falling into a well-researched class of universal algebraic operations. This class contains operations with "no ability to count". In contrast, functions like the parity function that have the ability to count are very input sensitive: their value changes even when the count changes only by one. In a far-reaching part of the algebraic theory the "no ability to count" class of operations generate algebras that "avoid types one and two" [HM88] congruences. This class of algebras have been recently characterized by local consistency checking algorithm, which was a breakthrough [BK09]. What makes the notion of StrongDem particularly attractive is that

when viewing its minimalistic definition, it seems a *necessary* condition for democracy, but it also has equivalent formulations, that are strong enough to accept it as a *sufficient* condition.

Definition 20 (Strong resilience). Let D be a finite domain and μ be a measure on D. The influence $\text{Inf}_{i,\mu}(f)$ of the i-th variable of $f : D^n \to D$ is $\text{Prob}_{\mu^{n+1}}(f(x) \neq f(x'))$, where x, x' run through all random input pairs that differ only in the i-th coordinate (μ^{n+1} gives a natural measure on such pairs). The maximal influence $\max \inf_\mu(f)$ is $\max_i \text{Inf}_{i,\mu}(f)$. A function $f : D^n \to D$ is strongly resilient if for every measure μ on D: $\max \inf_\mu(f^k) \to 0$ when $k \to \infty$ where f^k is defined recursively by composition $f^k = f(f^{k-1}, \dots, f^{k-1})$.

Theorem 38 (G. Kun and M. Szegedy [KS09]). *The following are equivalent:*

1. *f is StrongDem.*

2. *There is a strongly resilient operation in $[\{f\}]$.*

13   Final notes and future research

Our translations yield further surprising findings. It turns out that Sen's famous theorem [Sen79] has a generalization readily taken off the shelve from [BP75, JCC98]:

Theorem 39. *If $X \subseteq \{0, 1\}^m$ is 2-decomposable and k is odd, then the majority function with k voters is an IIA aggregator for X. For $k = $ odd the converse also holds.*

From this Sen's original theorem easily follows. In this work we have only started to elaborate on the close connection between Judgment Aggregation (more generally, Evaluation Aggregation) and universal algebra. There are several other ramifications of the connection: robustness results, extra conditions. In a follow-up result [SX14], we deal with the majoritarian aggregators.

14   Acknowledgements

References

[Arr50]   Kenneth J. Arrow. A Difficulty in the Concept of Social Welfare. *Journal of Political Economy*, 58(4):328–346, August 1950.

[BJ03]   Andrei A. Bulatov and Peter Jeavons. An Algebraic Approach to Multi-sorted Constraints. In *CP*, pages 183–198, 2003.

[BJK05]   Andrei A. Bulatov, Peter Jeavons, and Andrei A. Krokhin. Classifying the Complexity of Constraints Using Finite Algebras. *SIAM J. Comput.*, 34(3):720–742, 2005.

[BK09]   L. Barto and M. Kozik. Constraint Satisfaction Problems of Bounded Width. In *Foundations of Computer Science, 2009. FOCS '09. 50th Annual IEEE Symposium on*, pages 595–603, Oct 2009.

[BP75]   KirbyA. Baker and AldenF. Pixley. Polynomial Interpolation and the Chinese Remainder Theorem for Algebraic Systems. *Mathematische Zeitschrift*, 143(2):165–174, 1975.

[Bul11]   Andrei A Bulatov. Complexity of Conservative Constraint Satisfaction Problems. *ACM Transactions on Computational Logic (TOCL)*, 12(4):24, 2011.

[Che09]   Hubie Chen. A Rendezvous of Logic, Complexity, and Algebra. *ACM Comput. Surv.*, 42(1):2:1–2:32, December 2009.

[DH10a]   Elad Dokow and Ron Holzman. Aggregation of Binary Evaluations. *Journal of Economic Theory*, 145(2):495–511, 2010.

[DH10b]   Elad Dokow and Ron Holzman. Aggregation of Non-Binary Evaluations. *Advances in Applied Mathematics*, 45(4):487–504, 2010.

[FF11]   Dvir Falik and Ehud Friedgut. An Algebraic Proof of a Robust Social Choice Impossibility Theorem. In *FOCS*, pages 413–422, 2011.

[FV98]   T. Feder and M. Vardi. The Computational Structure of Monotone Monadic SNP and Constraint Satisfaction: A Study through Datalog and Group Theory. *SIAM Journal on Computing*, 28(1):57–104, 1998.

[Gei68]   D. Geiger. Closed Systems of Functions and Predicates. *Pacific Journal of Mathematics*, 27:95–100, 1968.

[HM88]   D. Hobby and R. McKenzie. The Structure of Finite Algebras. *Contemporary Mathematics*, 76, 1988.

[JCC98]   Peter Jeavons, David A. Cohen, and Martin C. Cooper. Constraints, Consistency and Closure. *Artif. Intell.*, 101(1-2):251–265, 1998.

[JCG97]   Peter Jeavons, David A. Cohen, and Marc Gyssens. Closure Properties of Constraints. *J. ACM*, 44(4):527–548, 1997.

[Jea98]   Peter Jeavons. On the Algebraic Structure of Combinatorial Problems. *Theor. Comput. Sci.*, 200(1-2):185–204, 1998.

[Kal02]   Gil Kalai. A Fourier-theoretic perspective on the Condorcet paradox and Arrow's theorem. *Advances in Applied Mathematics*, 29(3):412 – 426, 2002.

[KS09]   Gábor Kun and Mario Szegedy. A New Line of Attack on the Dichotomy Conjecture. In *STOC*, pages 725–734, 2009.

[LP02]   Christian List and Philip Pettit. Aggregating Sets of Judgments: An Impossibility Result. *Economics and Philosophy*, 18(1):89–110, 2002.

[NP02]   K Nehring and Clemens Puppe. Strategy-proof social choice on single-peaked domains: possibility, impossibility and the space between. *Unpublished manuscript, Department of Economics, University of California at Davis*, 2002.

[RF86]   Ariel Rubinstein and Peter C Fishburn. Algebraic Aggregation Theory. *Journal of Economic Theory*, 38(1):63 – 77, 1986.

[Sen79]   Amartya Sen. Personal Utilities and Public Judgements: Or What's Wrong With Welfare Economics. *The Economic Journal*, 89(355):pp. 537–558, 1979.

[SX14]   Mario Szegedy and Yixin Xu. Algebraic Theory of Majoritarian Aggregators. *in preparation*, 2014.

[TSSW96] L. Trevisan, G.B. Sorkin, M. Sudan, and D.P. Williamson. Gadgets, Approximation, and Linear Programming. In *Foundations of Computer Science, 1996. Proceedings., 37th Annual Symposium on*, pages 617–626, Oct 1996.

[Wil75]   Robert Wilson. On the Theory of Aggregation. *Journal of Economic Theory*, 10(1):89 – 99, 1975.